Counter-Competitor Intelligence: Applying the DOD Model to the Commercial Sector©

Session: Technical and Policy Focus Groups

Howard B. Low
Aegis Research Corporation
Space Engineering Center
1551 Vapor Trail
Colorado Springs, CO 80916
(719) 570-7041/567-9946
Fax (719) 570-7689/567-9898
E-mail: lowhowab@fafb.af.mil, hblow@pcisys.net

Counter-Competitor Intelligence: Applying the DOD Model to the Commercial Sector ©

Good Morning. I am Bruce Low from Aegis Research Corporation. My topic has to do with one of today's hottest items in the security arena – how to defend yourself against the well organized and pervasive competitor intelligence threat.

Competitor intelligence (CI) is becoming a well understood problem – it's even making headlines in the popular press. There's a growing general awareness that it can be the basis for coordinated attacks against a business on several fronts, generally focusing on reasonably mundane activities to discover proprietary confidences (such as new product release timing, key supplier identification, or hiring campaigns targeting your key personnel). However, it can also extend to much more hostile activities, like trying to buy trade secrets by suborning employees or supporting takeover attempts. The quantity and quality of sensitive information that can be collected to further these goals has only recently gotten the serious attention of a whole new generation of executives.

What's *not* well understood is how to defend against a competitor's intelligence attack. Designing and implementing a sound program may be difficult for a company wanting to protect itself after realizing how good competitor intelligence organizations can be.

In the past, unless you were in one of the few industries that maintained an active defense, protecting proprietary information was the purview of the corporate legal department, with minor support from the security division. The defense strategy focused almost entirely on threatening employees with dire legal consequences if they didn't adequately protect their company's secrets. That approach will no longer suffice.

Analyzing the changing environment and marketplace pressures and determining that you need to take action to protect yourself are the all-important first steps, but they are just the beginning. The follow-on problem comes in designing and implementing a fully integrated program that responds to your needs analysis and fits your specific requirements.

There's very little training available to upgrade the skills of the existing security staff or executive team. How is a company going to develop this modern defense-in-depth? Where will they find the expertise? What is the answer to this dilemma?

One solution is to recruit one of the few successful practitioners from one of the leading edge industries with effective counter-competitor intelligence programs. This can be a very expensive solution that will only pay dividends once that person creates his own infrastructure within the company to implement his program, which can take a large budget and one to two years.

Another way to gain rapid expertise at a more reasonable price, possibly in conjunction with a hiring and training campaign, is to outsource - hiring consultants to rapidly set up and maintain your program. We're probably not talking about the same company that provides your guard service, although they will play a support role in the final plan, as will Legal and Human Resources. The best qualified teams come from the small number of providers whose staffs have the necessary operations, legal, security and counterintelligence skills to address the full range of

disciplines required to defeat an aggressive competitor intelligence program (one that may even extend into corporate espionage and dirty tricks). These companies usually have strong teams of former Federal Government experts who gained their experience in the most aggressive competitor intelligence environment ever known – the Cold War!

A fully integrated counter-competitor intelligence program may be time consuming and difficult to implement, but the concept is easy to explain. Today's talk will focus on just such a concept – taking advantage of the risk-management methodology used on one of the Air Force's space programs, combining that approach with classic commercial practices currently in use.

The basics of this program are described in the following five step process.

- ***What*** do I protect? This is the most important step in the entire methodology. It defines the extent of the program by identifying those pieces of information that are so critical to our customer that he is willing to invest in a counter-competitor intelligence program to protect them.

The entire process is driven by the results of this analysis. This information is derived by one of several means. The quickest start up comes about if the customer has already identified the key facts that make him successful (based on a good understanding of his industry and knowing what information he needs to withhold from his competitors to keep them from overtaking him). This information comes from years of experience and lots of lessons learned the hard way. The driving force is that the customer has probably lost money in the past - customers and market share, critical design data, etc. – because he didn't protect himself from his competitors.

Lacking this foreknowledge, it's possible to develop these facts by a rigorous examination of the customer's business in the context of it's specific industry, maybe even hiring a competitor-intelligence company to tell him about himself. For example, is the product generally undifferentiated except for selling price, making production cost control information very important? Is the product's performance superior to others because of a secret design? Is a proprietary formula for the product responsible to strong sales, etc.? Defining both the categories and details of this critical information drives all the steps that follow. We can then derive who might want to collect the information and when and where it can be collected.

Clearly defining what you decide to protect is also an important step in any future legal actions against insider theft of trade secrets or other acts of corporate espionage under older statutes, as well as the more recent *Economic Espionage Act of 1996*. These laws require that information that a company might want to protect be clearly identified to employees charged with its protection. It also puts ethical competitor intelligence collectors (as well as corporate spies) on notice when viewing a clearly marked trade secret or piece of proprietary information.

- ***Why*** do I protect specific pieces of information? This step is a criticality analysis.

We will adapt one of the two basic approaches of military weapons system criticality analysis as the basis for this step. That approach questions, "Can the enemy use this information to copy the weapon system?". In our commercial example, the general equivalent, "Can the information be used to copy my product/process/etc.?" has clear application. The second half of this basic question goes to the discovery of related information. The answer to these questions in the defense world are further analyzed to define *how critical* the information might be, and then assigning a classification of Top Secret, Secret, Confidential, and even Unclassified But

Sensitive, depending on the degree of damage that would occur if the information were compromised.

The corporate world could easily follow that model, even using the same notations, e.g., "XYZ Corporation TOP SECRET". In our example, we might end up protecting information about a product's engineering, design, materials, components, manufacturing processes, unit costs, and marketing strategies and release dates all at different levels of 'classification'. In fact, the legal team would be happy to have our proprietary information this well defined because it makes it easier to assign damages in actionable cases.

The second basic military question, "Can this information be used to defeat my weapon system?" has less clear application, but we still need to perform this analysis so that we know about our vulnerabilities. At the minimum, a competitor might use this information for negative advertising. Worst case, this information can support a 'dirty tricks' campaign (e.g., it could be disastrous if a competitor drives up the price of a component in critically short supply).

- ***Who*** do I protect my critical information from?

The commercial marketplace is very different from the national security environment. Almost all of the threat comes from traditional business analysts using publicly available information. The threat from corporate espionage and foreign government intelligence services cooperating with a competitor is comparatively small (although on the rise – more about that later). The *who* is therefore the overt competitor intelligence community, ranging from 1-man shops simply cruising the Internet, to the very large multinational companies using sophisticated research tools to acquire every shred of relevant information in the public domain, no matter how obscure the source.

This doesn't mean that government sponsored intelligence doesn't happen, and that the information is not passed to foreign corporate competitors! Unlike this country, certain nations do share intelligence with their industries, especially when that industry is partially or wholly owned by that foreign government! To quote the National CounterIntelligence Center's (NACIC) 1997 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, "the theft, misappropriation, wrongful receipt, transfer, and/or use of US trade secrets and other economic information, particularly by foreign governments and their agents or instrumentalities, poses a direct threat to the health and competitiveness of the US economy".

If your business has foreign competitors who fit this scenario and it is likely that a foreign government is going to attack your security program, you will require the assistance of the Federal government to defeat them. Our government may find out about the attack before you do (through classified intelligence sources and methods) and come to you to arrange for a joint commercial-government response. Or, you might suspect that you're under attack by a foreign intelligence service and go to the government to get expert help dealing with threat.

Defining which threat applies to you requires analysis of the specific marketplace and the forces at work driving the competitor intelligence/foreign intelligence service effort. A multinational client protecting information about a revolutionary product in a very competitive defense market segment having major repercussions on his competitors, as well as impacts on his own share price on the stock market, can expect to be attacked by the professional competitor intelligence collection community, the internal competitor

intelligence departments of individual competitors, and probably foreign government intelligence services. To quote the NACIC report again, "A 1996 Defense Investigative Service summary of foreign contacts indicated that numerous foreign countries displayed some type of suspicious interest in one or more of the 18 technology categories listed in the Military Critical Technology List (MCTL), which is published by the Department of Defense. These major technology categories include:

- Aeronautics systems.
- Armaments and energetic materials.
- Chemical and biological systems.
- Directed and kinetic energy systems.
- Electronics.
- Ground systems.
- Guidance, navigation, and vehicle control.
- Information systems.
- Information warfare.
- Manufacturing and fabrication.
- Marine systems.
- Materials
- Nuclear systems.
- Power systems.
- Sensors and lasers.
- Signature control.
- Space systems.
- Weapons effects and countermeasures."

On the other hand, there are many cases where information requirements are simpler, and the collection threat might be limited to competitors trying to anticipate each others' local marketing campaigns. For example, how much do you think Earl Scheib® spends to find out about what Maaco® is up to, and who do you think they hire to do the work? Probably not too much, and what they *are* interested in can be collected fairly easily by legal and ethical means.

Finally, let's clear up any potential confusion between protecting proprietary information from competitors and hiding information that is required to be filed for some statutory purpose from U.S. government entities. We oppose using a counter-competitor intelligence program to achieve illegal ends.

- ***When*** and ***where*** do I protect my critical information? *Exposure analysis* is the next step.

Exposure analysis looks at the prioritized list of information that requires protection, focusing on the most important first, and determines when and where that information is susceptible to collection, either in its final form, or as uncollated bits and pieces. An example of the former might be a carefully controlled final report to the Board of Directors that summarizes very sensitive line item costs in a product line. Using our example, "uncollated bits and pieces" are then the extra copies of individual bills from suppliers that go into the dumpster outside the fence.

These analyses also includes the collection of second order facts that can be used to derive protected information through analysis of what the military calls *indicators*. A good example of this might be spectroradiometric analysis of legally collected airborne effluents to detect chemical by-products that help a competitor understand your manufacturing process. A simpler example might be the number of cars in your factory's parking lot during the 2nd and 3rd shifts to help determine production output.

- ***How*** do I protect this information? Here were consider the full range of *countermeasures* available to defeat an intelligence attack.

The actions you take to protect yourself, based on the cumulative results of the *what*, *who*, *when* and *where* analyses, will include a combination of manufacturing and operations, administrative, legal, financial and security activities. The specific mix of countermeasures is tailored for each problem.

For example, traditional DOD counterintelligence, operations and communications security (OPSEC and COMSEC), and physical security countermeasure are effective against illegal and unethical corporate espionage methods, computer penetration, and other specialized technical operations, extending to foreign government-sponsored communications intercept and human intelligence (HUMINT) operations. On the other hand, limiting the damaged caused by legal research by industry experts using sophisticated tools may require more creative responses so that the security program doesn't get in the way of the overriding business interests of the customer.

There are dozens of tools on the full menu of countermeasure options, and they must be integrated through a master plan. Some are relatively simple to put in place, but others require specialized training to plan and implement. All have to be monitored (once in place) and fine-tuned to insure that they remain effective.

The bottom line is to plan carefully to protect your secrets: a poorly designed and executed counter-competitor intelligence protection plan is not only a waste of money, the resulting false sense of security will significantly increase the risk of losing the information you most want to protect!

Remember... once compromised, secrets aren't!

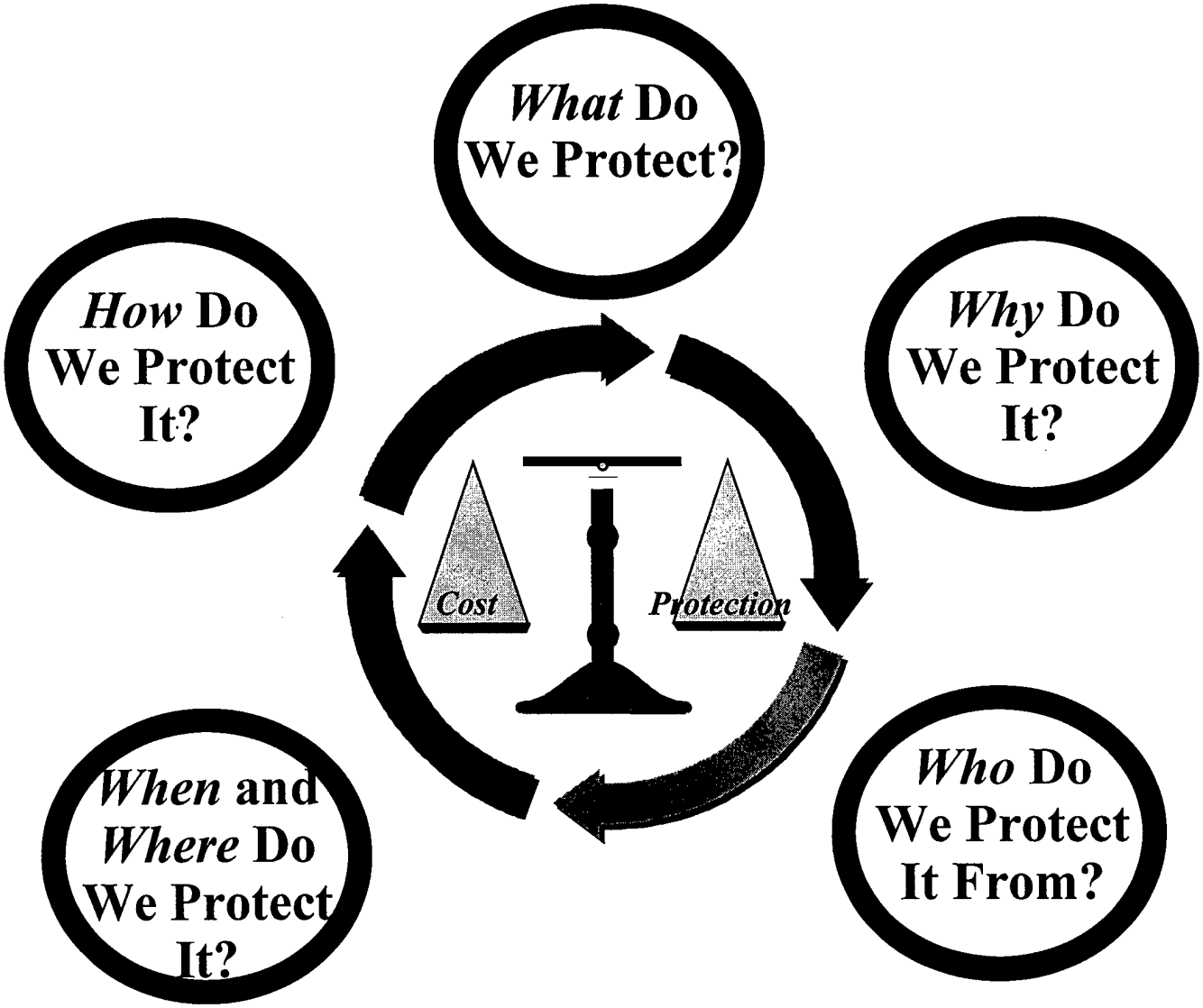
- END -

Aegis Research Corporation

©Howard B. Low 1998
Aegis Research Corporation, Space Engineering Center
1551 Vapor Trail, Colorado Springs, CO 80916
(719) 570-7041/567-9946 Fax (719) 570-7689/567-9898
E-mail: hblow@pcisys.net, lowhowab@fafb.af.mil

Counter-Competitor Intelligence:

Applying the DOD Model to the Commercial Sector©



Protection Planning Cycle